**Statement for the Record**
**Michael A. Vatis**
**Director, National Infrastructure Protection Center**
**Federal Bureau of Investigation**
**before the**
**Senate Committee on Commerce, Science and Transportation**
**Subcommittee on Communications**

Washington, D. C.
March 8, 2000

## Introduction

Mr. Chairman, Senator Hollings, and Members of the Subcommittee: Thank you for inviting me to discuss the threats to our Nation=s critical infrastructures and the NIPC=s approach to meeting those challenges. In 1998 the National Infrastructure Protection Center (NIPC) was established as a focal point for the federal government's efforts to protect the critical infrastructures. Much has happened since then to demonstrate both the wisdom of establishing such a Center and the seriousness of the problem it was designed to address. In the last two years we have seen the spread of destructive computer viruses affecting millions of users, a major international intrusion into government computer networks, and denial-of-service attacks against some of the most popular e-commerce websites. Today I will focus on the nature of the national security and criminal threats we face in cyberspace, the progress we have made with our interagency partners in meeting those threats, and the continuing challenges we face.

## The NIPC

The NIPC is an interagency Center located at the FBI. Created in 1998, the NIPC serves as the focal point for the government's efforts to warn of and respond to cyber attacks, particularly those that are directed at our nation=s Acritical infrastructures.@ These infrastructures include telecommunications and information, energy, banking and finance, transportation, government operations, and emergency services. In Presidential Decision Directive (PDD) 63, the President directed that the NIPC serve as a Anational critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity.@ The PDD further states that the mission of the NIPC Awill include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response.@

To accomplish its goals, the NIPC is organized into three sections:

The Computer Investigations and Operations Section (CIOS) is the operational response arm of the Center. It supports and, where necessary, coordinates computer investigations conducted by FBI field offices and other agencies throughout the country, provides expert technical assistance to

network investigations, and provides a cyber emergency response capability to coordinate the response to a national-level cyber incident.

The Analysis and Warning Section (AWS) serves as the "indications and warning@ arm of the NIPC. It provides tactical analytical support during a cyber incident, and also develops strategic analyses of threats for dissemination to both government and private sector entities so that they can take appropriate steps to protect themselves.. Through its 24/7 watch and warning operation, it maintains a real-time situational awareness by reviewing numerous governmental and Aopen@ sources of information and by maintaining communications with partner entities in the government and private sector. Through its efforts, the AWS strives to acquire indications of a possible attack, assess the information, and issue appropriate warnings to government and private sector partners as quickly as possible

The Training, Outreach and Strategy Section (TOSS) coordinates the vital training of cyber investigators in the FBI field offices, other federal agencies, and state and local law enforcement. It also coordinates outreach to private industry and government agencies to build the partnerships that are key to both our investigative and our warning missions. In addition, this section manages our efforts to catalogue information about individual Akey assets@ across the country which, if successfully attacked, could have significant repercussions on our economy or national security. Finally, the TOSS handles the development of strategy and policy in conjunction with other agencies and the Congress.

Beyond the NIPC at FBI Headquarters, we have also created a cyber crime investigative program in all FBI Field Offices called the National Infrastructure Protection and Computer Intrusion (NIPCI) Program. This program, managed by the NIPC, consists of special agents in each FBI Field Office who are responsible for investigating computer intrusions, viruses, or denial of service attacks, for implementing our key asset initiative, and for conducting critical liaison activities with private industry. They are also developing cyber crime task forces in partnership with state and local law enforcement entities within their jurisdiction to leverage the limited resources in this area.

**The Broad Spectrum of Threats**

Over the past several years we have seen a wide range of cyber threats ranging from defacement of websites by juveniles to sophisticated intrusions that we suspect may be sponsored by foreign powers, and everything in between. Some of these are obviously more significant than others. The theft of national security information from a government agency or the interruption of electrical power to a major metropolitan area would have greater consequences for national security, public safety, and the economy than the defacement of a web-site.

But even the less serious categories have real consequences and, ultimately, can undermine confidence in e-commerce and violate privacy or property rights. A web site hack that shuts down an e-commerce site can have disastrous consequences for a business. An intrusion that results in the theft of credit card numbers from an online vendor can result in significant financial loss and, more broadly, reduce consumers= willingness to engage in e-commerce. Recent surveys confirm this point. According

to a poll of Internet users by PC Data Online, 90% of those surveyed are concerned about the recent denial of service attacks. One in three surveyed said they were affected by the DDOS attacks. Further, over 40% of those surveyed said that they would be less likely to send credit card information over the Internet in the future.

Such surveys demonstrate the simple fact that the Internet has become a major aspect of everyday life for many Americans and is fast becoming a major part of our economy. There were over 100 million Internet users in the United States in 1999. That number is projected to reach 177 million in the United States and 502 million worldwide by the end of 2003. Electronic commerce has emerged as a new sector of the American economy, accounting for over $100 billion in sales during 1999, more than double the amount in 1998. By 2003, electronic commerce is projected to exceed $1 trillion. It should be no surprise, then, that as Internet use and e-commerce continue to grow at a rapid pace, the rate of cyber crime is also rising dramatically.

A significant part of the problem is the lack of adequate security on the Internet. As Lou Gerstner, the CEO of IBM said in a speech at Boston College on Monday, ANo brick-and-mortar company would ever consider opening its doors without locks, video cameras and a security staff. Yet every day hundreds of Web enterprises do just that.@ A fundamental need, therefore, is to raise the level of security on the Internet. This is clearly the role of the private sector. The government has neither the responsibility nor the expertise to act as the private sector=s system administrator. We can help, however, by providing information to the private sector about concrete threats and the latest techniques being utilized by cyber criminals, so that private companies can take steps to secure their systems against those threats. We also need to ensure that law enforcement has the capabilities to investigate cyber crime that does occur.

The following are some of the categories of cyber threats that we confront today.

*Insiders.* The disgruntled insider (a current or former employee of a company) is a principal source of computer crimes for many companies. Insiders= knowledge of the target companies= network often allows them to gain unrestricted access to cause damage to the system or to steal proprietary data. The 1999 Computer Security Institute/FBI report notes that 55% of respondents reported malicious activity by insiders.

One example of an insider was George Parente. In 1997, Parente was arrested for causing five network servers at the publishing company Forbes, Inc., to crash. Parente was a former Forbes computer technician who had been terminated from temporary employment. In what appears to have been a vengeful act against the company and his supervisors, Parente dialed into the Forbes computer system from his residence and gained access through a co-worker's log-in and password. Once online, he caused five of the eight Forbes computer network servers to crash, and erased all of the server volume on each of the affected servers. No data could be restored. Parente's sabotage resulted in a two day shut down in Forbes' New York operations with losses exceeding $100,000. Parente pleaded guilty to one count of violating of the Computer Fraud and Abuse Act, Title 18 U.S.C. 1030.

*Hackers*. Hackers (or Acrackers@) are also a common threat. They sometimes crack into networks simply for the thrill of the challenge or for bragging rights in the hacker community. Recently, however, we have seen more cases of hacking for illicit financial gain or other malicious purposes. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the World Wide Web and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use. The distributed denial-of-service (DDOS) attacks earlier this month are only the most recent illustration of the economic disruption that can be caused by tools now readily available on the Internet.

We have also seen a rise recently in politically motivated attacks on web pages or email servers, which some have dubbed "hacktivism. In these incidents, groups and individuals overload e-mail servers or deface web sites to send a political message. While these attacks generally have not altered operating systems or networks, they have disrupted services, caused monetary loss, and denied the public access to websites containing valuable information, thereby infringing on others' rights to disseminate and receive information.

*Virus Transmitters*. Virus transmitters are posing an increasingly serious threat to networks and systems worldwide. Last year saw the proliferation of several destructive computer viruses or A worms,@ including the Melissa Macro Virus, the Explore.Zip worm, and the CIH (Chernobyl) Virus. The NIPC frequently sends out warnings or advisories regarding particularly dangerous viruses, which can allow potential victims to take protective steps and minimize the destructive consequences of a virus.

The Melissa Macro Virus was a good example of our two-fold response -- encompassing both warning and investigation -- to a virus spreading in the networks. The NIPC sent out warnings as soon as it had solid information on the virus and its effects; these warnings helped alert the public and reduce the potential destructive impact of the virus. On the investigative side, the NIPC acted as a central point of contact for the field offices who worked leads on the case. A tip received by the New Jersey State Police from America Online, and their follow-up investigation with the FBI's Newark Division, led to the April 1, 1999 arrest of David L. Smith. Mr. Smith pleaded guilty to one count of violating 18 U.S.C. ' 1030 in Federal Court, and to four state felony counts. As part of his guilty plea, Smith stipulated to affecting one million computer systems and causing $80 million in damage. Smith is awaiting sentencing.

*Criminal Groups*. We are also seeing the increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain. In September, 1999, two members of a group dubbed the "Phonemasters" were sentenced after their conviction for theft and possession of unauthorized access devices (18 USC ' 1029) and unauthorized access to a federal interest computer (18 USC ' 1030). The "Phonemasters" were an international group of criminals who penetrated the computer systems of MCI, Sprint, AT&T, Equifax, and even the National Crime Information Center. Under judicially approved electronic surveillance orders, the FBI's Dallas Division made use of new

data intercept technology to monitor the calling activity and modem pulses of one of the suspects, Calvin Cantrell. Mr. Cantrell downloaded thousands of Sprint calling card numbers, which he sold to a Canadian individual, who passed them on to someone in Ohio. These numbers made their way to an individual in Switzerland and eventually ended up in the hands of organized crime groups in Italy. Cantrell was sentenced to two years as a result of his guilty plea, while one of his associates, Cory Lindsay, was sentenced to 41 months.

The Phonemasters= methods included "dumpster diving" to gather old phone books and technical manuals for systems. They used this information to trick employees into giving up their logon and password information. The group then used this information to break into victim systems. It is important to remember that often "cyber crimes" are facilitated by old fashioned guile, such as calling employees and tricking them into giving up passwords. Good cyber security practices must therefore address personnel security and "social engineering" in addition to instituting electronic security measures.

Another example of cyber intrusions used to implement a criminal conspiracy involved Vladimir L. Levin and numerous accomplices who illegally transferred more than $10 million in funds from three Citibank corporate customers to bank accounts in California, Finland, Germany, the Netherlands, Switzerland, and Israel between June and October 1994. Levin, a Russian computer expert, gained access over 40 times to Citibank's cash management system using a personal computer and stolen passwords and identification numbers. Russian telephone company employees working with Citibank were able to trace the source of the transfers to Levin's employer in St. Petersburg, Russia. Levin was arrested in March 1995 in London and subsequently extradited to the U.S. On February 24, 1998, he was sentenced to three years in prison and ordered to pay Citibank $240,000 in restitution. Four of Levin's accomplices pleaded guilty and one was arrested but could not be extradited. Citibank was able to recover all but $400,000 of the $10 million illegally transferred funds.

Unfortunately, cyberspace provides new tools not only for criminals, but for national security threats as well. These include terrorists, foreign intelligence agencies, and foreign militaries. Director of Central Intelligence George Tenet testified in February 2000, before the Senate Armed Services Committee, that many of the tools and weapons that can be used for information warfare purposes are Aavailable on the open market at relatively little cost.@ The DCI went on to note that the critical threat of IW lies in its potential as a Aforce multiplier@ for an adversary of the United States.

Three major categories of threat actors pose a national security challenge to the United States in cyber space.

*Terrorists.* Terrorists groups are increasingly using new information technology and the Internet to formulate plans, raise funds, spread propaganda, and to communicate securely. In his statement on the worldwide threat in 2000, Director of Central Intelligence George Tenet testified that terrorists groups, Aincluding Hizbollah, HAMAS, the Abu Nidal organization, and Bin Ladens al Qa=ida organization are using computerized files, e-mail, and encryption to support their operations.@ In one example, convicted terrorist Ramzi Yousef, the mastermind of the World Trade Center bombing, stored

detailed plans to destroy United States airliners on encrypted files on his laptop computer. While we have not yet seen these groups employ cyber tools as a *weapon* to use against critical infrastructures, their reliance on information technology and acquisition of computer expertise are clear warning signs. Moreover, we have seen other terrorist groups, such as the Internet Black Tigers (who are reportedly affiliated with the Tamil Tigers), engage in attacks on foreign government web-sites and email servers. A Cyber terrorism@ B by which I mean the use of cyber tools to shut down critical national infrastructures (such as energy, transportation, or government operations) for the purpose of coercing or intimidating a government or civilian population B is thus a very real, though still largely potential, threat.

*Foreign intelligence services*. Not surprisingly, foreign intelligence services have adapted to using cyber tools as part of their espionage tradecraft. Even as far back as 1986, before the worldwide surge in Internet use, the KGB employed West German hackers to access Department of Defense systems in the well-known ACuckoo=s Egg@ case. While I cannot go into specifics about more recent developments in an open hearing, it should not surprise anyone to hear that foreign intelligence services increasingly view computer intrusions as a useful tool for acquiring sensitive U.S. government and private sector information.

*Information Warfare*. The prospect of "information warfare" by foreign militaries against our critical infrastructures is perhaps the greatest potential cyber threat to our national security. We know that several foreign nations are developing information warfare doctrine, programs, and capabilities for use against the United States or other nations. Knowing that they cannot match our military might with conventional or Akinetic@ weapons, nations see cyber attacks on our critical infrastructures or military operations as a way to hit what they perceive as America=s Achilles heel B our growing dependence on information technology in government and commercial operations. For example, two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counterbalance the military power of the United States. And a Russian official has also commented that an attack on a critical infrastructure could, "by virtue of its catastrophic consequences, completely overlap with the use of [weapons] of mass destruction."

**Distributed Denial of Service Tools**

The recent distributed denial of service(DDOS) attacks on e-commerce sites have garnered a tremendous amount of interest in the public and in the Congress. While we do not yet have official damage estimates, the Yankee Group, a research firm, estimates the impact of the attacks at $1.2 billion due to lost capitalization losses, lost revenues, and security upgrades. Because we are actively investigating these attacks, I cannot provide a detailed briefing on the status of our efforts. However, I can provide an overview of our activities to deal with the DDOS threat beginning last year and of our investigative efforts over the last three weeks. These attacks illustrate the growing availability of destructive, yet easy-to-use, exploits that are widely available on the Internet. They also demonstrate the NIPC=s two-fold mission: sharing information with the private sector and warning of possible threats, and responding to actual attacks.

In the fall of last year, the NIPC began receiving reports about a new set of Aexploits@ or attack tools collectively called distributed denial of service (or DDOS) tools. DDOS variants include tools known as ATrin00,@ ATribal Flood Net@ (TFN), ATFN2K,@ and AStacheldraht@ (German for Abarbed wire@). These tools essentially work as follows: hackers gain unauthorized access to a computer system(s) and place software code on it that renders that system a Amaster@ (or a Ahandler@). The hackers also intrude into other networks and place malicious code which makes those systems into agents (also known as Azombies@ or Adaemons@ or Aslaves@). Each Master is capable of controlling multiple agents. In both cases, the network owners normally are not aware that dangerous tools have been placed and reside on their systems, thus becoming third-party victims to the intended crime.

The "Masters" are activated either remotely or by internal programming (such as a command to begin an attack at a prescribed time) and are used to send information to the agents, activating their DDOS ability. The agents then generate numerous requests to connect with the attack=s ultimate target(s), typically using a fictitious or "spoofed" IP (Internet Protocol) address, thus providing a falsified identity as to the source of the request. The agents act in unison to generate a high volume of traffic from several sources. This type of attack is referred to as a SYN flood, as the SYN is the initial effort by the sending computer to make a connection with the destination computer. Due to the volume of SYN requests the destination computer becomes overwhelmed in its efforts to acknowledge and complete a transaction with the sending computers, degrading or denying its ability to complete service with legitimate customers **B** hence the term "Denial of Service". These attacks are especially damaging when they are coordinated from multiple sites **B** hence the term Distributed Denial of Service.

An analogy would be if someone launched an automated program to have hundreds of phone calls placed to the Capitol switchboard at the same time. All of the good efforts of the staff would be overcome. Many callers would receive busy signals due to the high volume of telephone traffic.

In November and December, the NIPC received reports that universities and others were detecting the presence of hundreds of agents on their networks. The number of agents detected clearly could have been only a small subset of the total number of agents actually deployed. In addition, we were concerned that some malicious actors might choose to launch a DDOS attack around New Year=s Eve in order to cause disruption and gain notoriety due to the great deal of attention that was being payed to the Y2K rollover. Accordingly, we decided to issue a series of alerts in December to government agencies, industry, and the public about the DDOS threat.

Moreover, in late December, we determined that a detection tool that we had developed for investigative purposes might also be used by network operators to detect the presence of DDOS agents or masters on their operating systems, and thus would enable them to remove an agent or master and prevent the network from being unwittingly utilized in a DDOS attack. Moreover, at that time there was, to our knowledge, no similar detection tool available commercially. We therefore decided to take the unusual step of releasing the tool to the Department of Defense, other government agencies, and to the public in an effort to reduce the level of the threat. We made the first variant of our software

available on the NIPC web site on December 30, 1999. To maximize the public awareness of this tool, we announced its availability in an FBI press release that same date. Since the first posting of the tool, we have posted three updated versions that have perfected the software and made it applicable to different operating systems.

The public has downloaded these tools tens of thousands of times from the web site, and has responded by reporting many installations of the DDOS software, thereby preventing their networks from being used in attacks and leading to the opening of criminal investigations both before and after the widely publicized attacks of the last few weeks. Our work with private companies has been so well received that the trade group SANS awarded their yearly Security Technology Leadership Award to members of the NIPC=s Special Technologies Applications Unit.

Last month, we received reports that a new variation of DDOS tools was being found on Windows operating systems. One victim entity provided us with the object code to the tool found on its network. On February 18 we made the binaries available to anti-virus companies (through an industry association) and the Computer Emergency Response Team (CERT) at Carnegie Mellon University for analysis and so that commercial vendors could create or adjust their products to detect the new DDOS variant. Given the attention that DDOS tools have received in recent weeks, there are now numerous detection and security products to address this threat, so we determined that we could be most helpful by giving them the necessary code rather than deploying a detection tool ourselves.

Unfortunately, the warnings that we and others in the security community had issued about DDOS tools last year, while alerting many potential victims and reducing the threat, did not eliminate the threat. Quite frequently, even when a threat is known and patches or detection tools are available, network operators either remain unaware of the problem or fail to take necessary protective steps. In addition, in the cyber equivalent of an arms race, exploits evolve as hackers design variations to evade or overcome detection software and filters. Even security-conscious companies that put in place all available security measures therefore are not invulnerable. And, particularly with DDOS tools, one organization might be the victim of a successful attack despite its best efforts, because another organization failed to take steps to keep itself from being made the unwitting participant in an attack.

On February 7, 2000, the NIPC received reports that Yahoo had experienced a denial of service attack. In a display of the close cooperative relationship that we have developed with the private sector, in the days that followed, several other companies (including Cable News Network, eBay, Amazon.com, Buy.com, and ZDNET), also reported denial of service outages to the NIPC or FBI field offices. These companies cooperated with us by providing critical logs and other information. Still, the challenges to apprehending the suspects are substantial. In many cases, the attackers used A spoofed@ IP addresses, meaning that the address that appeared on the target=s log was not the true address of the system that sent the messages. In addition, many victims do not keep complete network logs.

The resources required in an investigation of this type are substantial. Companies have been

victimized or used as Ahop sites@ in numerous places across the country, meaning that we must deploy special agents nationwide to work leads. We currently have seven FBI field offices with cases opened and all the remaining offices are supporting the offices that have opened cases. Agents from these offices are following up literally hundreds of leads. The NIPC is coordinating the nationwide investigative effort, performing technical analysis of logs from victims sites and Internet Service Providers (ISPs), and providing all-source analytical assistance to field offices. Moreover, parts of the evidentiary trail have led overseas, requiring us to work with our foreign counterparts in several countries through our Legal Attaches (Legats) in U.S. embassies.

While the crime may be high tech, investigating it involves a substantial amount of traditional investigative work as well as highly technical work. Interviews of network operators and confidential sources can provide very useful information, which leads to still more interviews and leads to follow-up. And victim sites and ISPs provide an enormous amount of log information that needs to be processed and analyzed by human analysts.

Despite these challenges, I am optimistic that the hard work of our agents, analysts, and computer scientists; the excellent cooperation and collaboration we have with private industry and universities; and the teamwork we are engaged in with foreign partners will in the end prove successful.

**Interagency Cooperation**

The broad spectrum of cyber threats described earlier, ranging from hacking to foreign espionage and information warfare, requires not just new technologies and skills on the part of investigators, but new organizational constructs as well. In most cyber attacks, the identity, location, and objective of the perpetrator are not immediately apparent. Nor is the scope of his attack -- i.e., whether an intrusion is isolated or part of a broader pattern affecting numerous targets. This means it is often impossible to determine at the outset if an intrusion is an act of cyber vandalism, organized crime, domestic or foreign terrorism, economic or traditional espionage, or some form of strategic military attack. The only way to determine the source, nature, and scope of the incident is to gather information from the victim sites and intermediate sites such as ISPs and telecommunications carriers. Under our constitutional system, such information typically can be gathered only pursuant to criminal investigative authorities. This is why the NIPC is part of the FBI, allowing us to utilize the FBI=s legal authorities to gather and retain information and to act on it, consistent with constitutional and statutory requirements.

But the dimension and varied nature of the threats also means that this is an issue that concerns not just the FBI and law enforcement agencies, but also the Department of Defense, the Intelligence Community, and civilian agencies with infrastructure-focused responsibility such as the Departments of Energy and Transportation. It also is a matter that greatly affects state and local law enforcement. This is why the NIPC is an interagency center, with representatives detailed to the FBI from numerous federal agencies and representation from state and local law enforcement as well. These representatives operate under the direction and authority of the FBI, but bring with them expertise and skills from their respective home agencies that enable better coordination and cooperation among all relevant agencies, consistent with applicable laws.

We have had many instances in the last two years where this interagency cooperation has proven critical. As mentioned earlier, the case of the Melissa virus was successfully resolved with the first successful federal prosecution of a virus propagator in over a decade because of close teamwork between the NIPCI squad in the FBI=s Newark Division and other field offices, the New Jersey State Police, and the NIPC.

The ASolar Sunrise@ case is another example of close teamwork with other agencies. In 1998, computer intrusions into U.S. military computer systems occurred during the Iraq weapons inspection crisis. Hackers exploited known vulnerabilities in Sun Solaris operating systems. Some of the intrusions appeared to be coming from the Middle East. The timing, nature, and apparent source of some of the attacks raised concerns in the Pentagon that this could be a concerted effort by Iraq to interfere with U.S. troop deployments. NIPC coordinated a multi-agency investigation which included the FBI, the Air Force Office of Special Investigations, the National Aeronautics and Space Administration, the Department of Justice, the Defense Information Systems Agency, the National Security Agency, and the Central Intelligence Agency. Within several days, the investigation determined that the intrusions were not the work of Iraq, but of several teenagers in the U.S. and Israel. Two juveniles in California pleaded guilty to the intrusions, and several Israelis still await trial. The leader of the Israeli group, Ehud Tenenbaum, has been indicted and is currently scheduled for trial in Israel in April.

More recently, we observed a series of intrusions into numerous Department of Defense and other federal government computer networks and private sector entities. Investigation last year determined that the intrusions appear to have originated in Russia. The intruder successfully accessed U.S. Government networks and took large amounts of unclassified but sensitive information, including defense technical research information. The NIPC coordinated a multi-agency investigation, working closely with FBI field offices, the Department of Defense, and the Intelligence Community. While I cannot go into more detail about this case here, it demonstrates the very real threat we face in the cyber realm, and the need for good teamwork and coordination among government agencies responsible for responding to the threat.

**Private Sector Cooperation**

Our success in battling cyber crime also depends on close cooperation with private industry. This is the case for several reasons. First, most of the victims of cyber crimes are private companies. Therefore, successful investigation and prosecution of cyber crimes depends on private victims reporting incidents to law enforcement and cooperating with the investigators. Contrary to press statements by cyber security companies that private companies won't share information with law enforcement, many private companies have reported incidents and threats to the NIPC or FBI field offices. The number of victims who have voluntarily reported DDOS attacks to us over the last few weeks is ample proof of this. While there are undoubtedly companies that would prefer not to report a crime because of fear of public embarrassment over a security lapse, the situation has improved markedly. Companies increasingly realize that deterrence of crime depends on effective law enforcement, and that the

long-term interests of industry depend on establishing a good working relationship with government to prevent and investigate crime.

Testimony two weeks ago before the Senate Appropriations Subcommittee for Commerce, State, and Justice by Robert Chesnut, Associate General Counsel for E-bay, illustrates this point:

> Prior to last week's attacks, eBay had established a close working relationship with the computer crimes squad within the Northern California office of the Federal Bureau of Investigation ("FBI"). E-Bay has long recognized that the best way to combat cyber crime, whether it's fraud or hacking, is by working cooperatively with law enforcement. Therefore, last year we established procedures for notifying the FBI in the event of such an attack on our web site. As result of this preparation, we were able to contact the FBI computer intrusion squad during the attack and provide them with information that we expect will assist in their investigation. In the aftermath of the attack, eBay has also been able to provide the FBI with additional leads that have come to our attention.

Second, the network administrator at a victim company or ISP is critical to the success of an investigation. Only that administrator knows the unique configuration of her system, and she typically must work with an investigator to find critical transactional data that will yield evidence of a criminal=s activity.

Third, the private sector has the technical expertise that is often critical to resolving an investigation. It would be impossible for us to retain experts in every possible operating system or network configuration, so private sector assistance is critical. In addition, many investigations require the development of unique technical tools to deal with novel problems. Private sector assistance has been critical there as well.

We have several other initiatives devoted to private sector outreach that bear mentioning here. The first is called AInfraGard.@ This is an initiative that we have developed in concert with private companies and academia to encourage information-sharing about cyber intrusions, exploited vulnerabilities, and physical infrastructure threats. A vital component of InfraGard is the ability of industry to provide information on intrusions to the local FBI field office using secure e-mail communications in both a "sanitized" and detailed format. The local FBI field offices can, if appropriate, use the detailed version to initiate an investigation; while NIPC Headquarters can analyze that information in conjunction with other information we obtain to determine if the intrusion is part of a broader attack on numerous sites. The NIPC can simultaneously use the sanitized version to inform other members of the intrusion without compromising the confidentiality of the reporting company. The key to this system is that whether, and what, to report is entirely up to the reporting company. A secure web site also contains a variety of analytic and warning products that we make available to the InfraGard community. The success of InfraGard is premised on the notion that sharing is a two-way street: the NIPC will provide threat information that companies can use to protect their systems, while companies will provide incident information that can be used to initiate an investigation and to warn

other companies.

Our Key Asset Initiative (KAI) is focused more specifically on the owners and operators of critical components of each of the infrastructure sectors. It facilitates response to threats and incidents by building liaison and communication links with the owners and operators of individual companies and enabling contingency planning. The KAI began in the 1980s and focused on physical vulnerabilities to terrorism. Under the NIPC, the KAI has been reinvigorated and expanded to focus on cyber vulnerabilities as well. The KAI currently involves determining which assets are key within the jurisdiction of each FBI Field Office and obtaining 24-hour points of contact at each asset in cases of emergency. Eventually, if future resources permit, the initiative will include the development of contingency plans to respond to attacks on each asset, exercises to test response plans, and modeling to determine the effects of an attack on particular assets. FBI field offices are responsible for developing a list of the assets within their respective jurisdictions, while the NIPC maintains the national database. The KAI is being developed in coordination with DOD and other agencies. Currently the database has about 2600 entries. This represents 2600 contacts with key private sector nodes made by the NIPC and FBI field offices.

A third initiative is a pilot program we have begun with the North American Electrical Reliability Council (NERC). Under the pilot program, electric utility companies and other power entities transmit cyber incident reports in near real time to the NIPC. These reports are analyzed and assessed to determine whether an NIPC warning, alert, or advisory is warranted. Electric power participants in the pilot program have stated that the information and analysis provided by the NIPC *back* to the power companies fully justify their participation in the program. It is our expectation that the Electrical Power Indications and Warning System will provide a full-fledged model for the other critical infrastructures.

Much has been said over the last few years about the importance of information sharing. Since our founding, the NIPC has been actively engaged in building concrete mechanisms and initiatives to make this sharing a reality, and we have built up a track record of actually sharing useful information. These efforts belie the notions that private industry won=t share with law enforcement in this area, or that the government won=t provide meaningful threat data to industry. As companies continue to gain experience in dealing with the NIPC and FBI field offices, as we continue to provide them with important and useful threat information, and as companies recognize that cyber crime requires a joint effort by industry and government together, we will continue to make real progress in this area.

**Meeting the Growing Cyber Threat**

As Internet use continues to soar, the number of cyber attacks is also increasing exponentially. Our case load reflects this growth. In FY 1998, we opened 547 computer intrusion cases; in FY 1999, that number jumped to 1154. Similarly, the number of pending cases increased from 206 at the end of FY 1997, to 601 at the end of FY 1998, to 834 at the end of FY 99, and to over 900 currently. These statistics include only computer intrusion cases, and do not account for computer facilitated crimes such as Internet fraud, child pornography, or e-mail extortion efforts. In these cases, the NIPC and NIPCI

squads often provide technical assistance to traditional investigative programs responsible for these categories of crime.

We can clearly expect these upward trends to continue, and for the threats to become more serious. While insiders, hackers, and criminal groups make up much of our case load at the moment,

c
w
w
w

w

Not only do investigators and analysts need the best equipment to conduct investigations in the rapidly evolving cyber system but the NIPC must be on the cutting edge of cyber research and development. Conducting a network intrusion or denial-of-service investigation often requires analysis of voluminous amounts of data. For example, one network intrusion case involving an espionage matter currently being investigated has required the analysis of 17.5 Terabytes of data. To place this into perspective, the entire collection of the Library of Congress, if digitized, would comprise only 10 Terabytes. The Yahoo DDOS attack involved approximately 630 Gigabytes of data, which is equivalent to enough printed pages to fill 630 pickup trucks with paper. Technical analysis requires high capacity equipment to store, process, analyze, and display data. Again, as the crime problem grows, we must ensure that our technical capacity keeps pace. We are also working closely with other agencies to ensure that we leverage existing resources to the fullest extent possible.

**Challenges in Combating Cyber Intrusions**

The burgeoning problem of cyber intrusions, viruses, and denial of service attacks poses unique challenges to the NIPC. These challenges require novel solutions, close teamwork among agencies and with the private sector, and adequate human and technical resources.

*Identifying the Intruder*. One major difficulty that distinguishes cyber threats from physical threats is determining who is attacking your system, why, how, and from where. This difficulty stems from the ease with which individuals can hide or disguise their tracks by manipulating logs and directing their attacks through networks in many countries before hitting their ultimate target. The "Solar Sunrise" case illustrates this point. This will continue to pose a problem as long as the Internet remains rife with vulnerabilities and allows easy anonymity and concealment.

*Jurisdictional Issues*. Another significant challenge we face is intrusions involving multiple jurisdictions. A typical investigation involves victim sites in multiple states and often many countries. This is the case even when the hacker and victim are both located in the United States. In the United States, we can subpoena records, engage in judicially approved electronic surveillance, and execute search warrants on suspects' homes, seize evidence, and examine it. We can do none of those things ourselves overseas; rather, we depend on the local authorities to assist us. In some cases the local police forces simply do not understand or cannot cope with the technology. In other cases, these nations simply do not have laws against computer intrusions and are therefore limited in their ability to help us. FBI Legal Attaches in 35 embassies abroad provide critical help in building bridges with local law enforcement to enhance cooperation on cyber crime and in working leads on investigations. As the Internet spreads to even more countries, we will see greater demands placed on the Legats to support computer crime investigations. The NIPC also has held international computer crime conferences and offered cyber crime training classes to foreign law enforcement officials to develop liaison contacts and bring these officials up to speed on cyber crime issues.

The most difficult situation will arise, however, in which a foreign country with interests adverse to our own simply refuses to cooperate. In such a situation, we could find that an investigation is

stymied unless we find an alternative method of tracing the activity back to its source.

**The Role of Law Enforcement**

Finally, I would like to conclude by emphasizing two key points. The first is that our role in combating cyber crime is essentially two-fold: (1) preventing cyber attacks before they occur or limiting their scope by disseminating warnings and advisories about threats so that potential victims can protect themselves; and (2) responding to attacks that do occur by investigating and identifying the perpetrator. This is very much an operational role. Our role is **not** to determine what security measures private industry should take, or to ensure that companies or individuals take them. It is the responsibility of industry to ensure that appropriate security tools are made available and are implemented. We certainly can assist industry by alerting them to the actual threats that they need to be concerned about, and by providing information about the exploits that we are seeing criminals use. But network administrators, whether in the private sector or in government, are the first line of defense.

Second, in gathering information as part of our warning and response missions, we rigorously adhere to constitutional and statutory requirements. Our conduct is strictly limited by the Fourth Amendment, statutes such as Title III and ECPA, and the Attorney General Guidelines. These rules are founded first and foremost on the protection of privacy inherent in our constitutional system. Respect for privacy is thus a fundamental guidepost in all of our activities.

**Conclusion**

I want to thank the subcommittee again for giving me the opportunity to testify here today. The cyber threat is real, multifarious, and growing. The NIPC is moving aggressively to meet this challenge by training investigators and analysts to investigate computer intrusion cases, equipping them with the latest technology, developing our analytic capabilities and warning mechanisms to head off or mitigate attacks, and closely cooperating with the private sector. We have already made considerable progress in developing our capabilities to protect public safety and national security in the Information Age. I look forward to working with Congress to ensure that we continue to be able to meet the threat as it evolves and grows. Thank you.